This paper is dedicated to Professor Wu WenTsün on his eightieth birthday

On the Theory of Resolvents and Its Applications

Xiao-Shan Gao
Institute of Systems Science
Academia Sinica
Beijing 100080, P.R. China
e-mail: xgao@mmrc.iss.ac.cn

Shang-Ching Chou
Department of Computer Science
The Wichita State University
Wichita, KS 67208, USA
e-mail: chou@cs.twsu.edu

Abstract

We extend the concept of the resolvent of a prime ideal to the concept of the resolvent of a general ideal with respect to a set of parameters and propose an algorithm to construct the generalized resolvents based on Wu-Ritt's zero decomposition algorithm. Our generalized algorithm has the following applications. (1) For a reducible variety V, we can find a direction on which V is projected birationally to an irreducible hypersurface. (2) We give a new algorithm to find a primitive element for a finite algebraic extension of a field of characteristic zero. (3) We present a complete method of finding parametric equations for algebraic curves. (4) We give a method of solving a system of polynomial equations to any given precision.

Keywords. Resolvents, parameterization of algebraic curves, primitive elements, polynomial equation solving, Wu-Ritt's decomposition algorithm.

1 Introduction

Some frequently used algebraic algorithms share the same property that they transform a set of polynomial equations to a single polynomial equation such that the zero set of the polynomial set and the hypersurface defined by the single polynomial are equivalent in certain sense. For algorithms with this property, we may mention: the algorithm to find a primitive element for a finitely generated algebraic extension field [17], the algorithm to find a plane curve which is birational to a space algebraic curve [1], etc. In this paper, we present a general algorithm which can be used to tale care of this kind of problems.

In Ritt's classical book *Differential Algebra* [19], an algorithm of constructing *resolvents* for a prime ideal is given. The hypersurface defined by a resolvent of a prime ideal is birational to the irreducible variety defined by the prime ideal. Hence by using Ritt's resolvent algorithm some of the problems mentioned in the above paragraph can be solved, e.g., we can construct a plane curve which is birational to a given irreducible algebraic curve. But Ritt's resolvent algorithm can not be used to the problem of finding primitive elements of a finitely generated algebraic extension field, because the polynomial equations giving the algebraic numbers generally might not consist of a prime ideal.

In this paper, we extend Ritt's concept of resolvent to general ideals with respect to (abbr. w.r.t) a parameter set. We also give an algorithm to construct a resolvent of an ideal w.r.t to a parameter set. The algorithm works as follows. We first compute a resolvent for each of the prime components of the ideal using Wu-Ritt's decomposition algorithm or Buchberger's Gröbner basis algorithm, then obtain the resolvent of the ideal from the resolvents of its prime components.

The generalized resolvent algorithm has the following applications:

(1) For a reducible variety V which is the union of irreducible varieties with the same dimension and the same parameter set, we can find a map to transform V into a hypersurface which is birational to V.

(2) As a special case of (1), we can find plane curves which are birational to a given algebraic curve. We also present a new algorithm to construct a set of parametric equations for a rational plane curve. Hence, we have a complete method to decide whether an algebraic curve is rational, and if it is, to find parametric equations for it.

(3) We give an algorithm to find a primitive element for a finite algebraic extension field of a field with characteristic zero. Probabilistic methods to construct a primitive element for a finitely generated algebraic extension field are given in [17, 25]. Our method in this paper is deterministic and applicable to more general cases: the generator sequence of the algebraic elements can be defined successively, i.e., an algebraic element in the sequence depends on the previous elements.

(4) In the work of solving polynomial equation systems, a typical method is first transforming the system into a triangular system and then solving the triangular system iteratively [23, 15]. But when one tries to solve a triangular form using numerical methods, we meet the following error estimation problem: For a triangular equation system

$$A_1(x_1) = 0, A_2(x_1, x_2) = 0, ..., A_p(x_1, ..., x_p) = 0$$

we ask what accuracy for x_1 is needed if we want a certain accuracy for x_p. In [2], this is considered to be an inherent difficulty of polynomial equation solving. In [14, 11], probabilistic methods based on the Gröbnr basis method to compute the roots of a polynomial set to any given precision are given. Using the method of resolvents, we can give a deterministic method. Since our method is based on the Wu-Ritt's characteristic method whose complexity is singly exponential [12], it is generally faster than the previously known methods based on Gröbner basis method whose complexity is doubly exponential.

The algorithm of constructing resolvents reported in this paper is used to factorize a polynomial over an algebraic extension field [26]. The factorization algorithm presented in [22] uses a technique similar to that of computing the resolvents.

The paper is organized as follows. In Section 2, we introduce some notions which are used in this paper. In Section 3, we prove the existence of the resolvents and present an algorithm to compute them. In Section 4, we show how to use the theory of resolvents to various problems.

2 Preliminaries on Wu-Ritt's Decomposition Algorithm

In this section, we introduce some concepts which will be used later. A detailed description of these concepts can be found in [23].

Let K be a computable field of characteristic zero and $K[x_1,...,x_n]$ or $K[X]$ be the ring of polynomials in the indeterminates $x_1,...,x_n$. Unless explicitly mentioned otherwise, all polynomials in this paper are in $K[X]$. Since K is of characteristic zero, we can assume that the field of rational numbers $\mathbf{Q}$ is a subfield of K.

For $P \in K[X]$, we can write $P = c_d x_p^d + ... + c_1 x_p + c_0$, where $c_i \in K[x_1,...,x_{p-1}]$. We call $c_d \neq 0$ the *initial* of P and p the *class* of P, or $init(P) = c_d$ and $class(P) = p$. If $P \in K$, $class(P) = 0$. For polynomials P and G with $class(P) > 0$, let $prem(G;P)$ be the *pseudo remainder* of G w.r.t P.

A sequence of polynomials $ASC = A_1,...,A_p$ is said to be an *ascending (*abbr. *asc) chain*, if either $r = 1$ and $A_1 \neq 0$ or $0 < class(A_i) < class(A_j)$ for $1 \le i < j$ and A_k is of higher degree than A_m for $m > k$ in x_{n_k} where $n_k = class(A_k)$.

For an asc chain $ASC = A_1,...,A_p$ such that $class(A_1) > 0$, we define the pseudo remainder of a polynomial G w.r.t ASC inductively as

$$prem(G;ASC) = prem(prem(G;A_p);A_1,...,A_{p-1}).$$

Let $R = prem(G;ASC)$. Then from the computation procedure of the pseudo division, we have the following important *remainder formula*:

$$JG = B_1A_1 + \ldots + B_pA_p + R \tag{2.1}$$

where J is a product of powers of the initials of the polynomials in ASC and the B_i are polynomials. For an asc chain ASC, we define

$$PD(ASC) = \{g \mid prem(g, ASC) = 0\}$$

By (2.1), a zero of ASC which does not annul the initials of the polynomial in ASC is a zero of $PD(ASC)$.

For an asc chain $ASC = A_1,...,A_p$, we always make a renaming of the variables. If A_i is of class m_i, we rename x_{m_i} as y_i, and the other variables are renamed as $u_1,...,u_q$, where $q = n-p$. The variables $u_1,...,u_q$ are called a *parameter set* of ASC. A polynomial in $K[u_1,...,u_q]$ is called a u-pol.

Let $ASC = A_1,...,A_p$ be an asc chain with $u_1,...,u_q$ as parameters. We will define when ASC is *irreducible*. For indeterminates $\tau_1,...,\tau_q$, let H_1 be the polynomial obtained from A_1 by replacing u_i by τ_i, $i = 1,...,q$. Then H_1 is a polynomial in $K_1[y_1]$ where $K_1 = K(\tau)$. We assume that H_1 is irreducible and let η_1 be a zero of H_1. Now let

$$\tau_1,...,\tau_q,\eta_1,...,\eta_{k-1} \tag{2.1.1}$$

be a set of zeros of $A_1, ..., A_{k-1}$ constructed as above. Let H_k be the polynomial obtained by replacing $u_1, ..., u_q, y_1, ..., y_{k-1}$ by (2.1.1). We assume that (2.1.1) is not a zero of the initial of A_k and H_k is an irreducible polynomial in $K_k[y_k]$ where $K_k = K_{k-1}(\eta_{k-1})$. Let η_k be a zero of H_k. Finally, we have the following quantities

$$\tau_1, ..., \tau_q, \eta_1, ..., \eta_{p-1}, \eta_p$$

which consist of a solution for the polynomials in ASC. If we can construct such a set of zeros according to the above procedure then ASC is said to be *irreducible* and the zero is called a *generic zero* of ASC. Since a generic zero of ASC does not annul the initials of the polynomials in ASC, by (2.1) it is a zero of $PD(ASC)$.

Definition 2.1. The dimension of an irreducible ascending chain $ASC = A_1, ..., A_p$ is defined to be $DIM(ASC) = n - p$.

Thus $DIM(ASC)$ is equal to the number of parameters of ASC.

Definition 2.2. *A characteristic set* (abbr. char set) of an ideal ID is an asc chain ASC in ID such that for all $P \in D$, $prem(P, ASC) = 0$.

Theorem 2.3. If ASC is an irreducible asc chain then $PD(ASC)$ is a prime ideal with dimension $DIM(ASC)$. Conversely, each char set of a prime ideal is an irreducible asc chain.

Proof. See [19] p88. ▮

Lemma 2.4. Let ASC be an irreducible asc chain with parameters $u_1, ..., u_q$. If Q is a polynomial not in $PD(ASC)$, then we can find a nonzero u-pol P such that $P \in Ideal(ASC, Q)$ (i.e., the ideal generated by Q and the polynomials in ASC).

Proof. See [23]. ▮

Lemma 2.5. Let ASC be an irreducible asc chain with parameters $u_1, ..., u_q$. We can find an irreducible asc chain ASC' and such that $PD(ASC) = PD(ASC')$ and the initials of the polynomials in ASC' are u-pols.

Proof. See [8]. ▮

Let PS be a polynomial set. For an algebraic closed extension field E of K, let

$$Zero(PS) = \{x = (x_1, ..., x_n) \in E^n \mid \forall P \in PS, P(x) = 0\}.$$

For two polynomial sets PS and DS, we define

$$Zero(PS/DS) = Zero(PS) - \cup_{d \in DS} Zero(d).$$

Then we have the following Wu-Ritt's decomposition algorithm.

Theorem 2.6. For finite polynomial sets PS and DS, we can either detect the emptiness of $Zero(PS/DS)$ or find irreducible asc chains ASC_i, $i = 1, ..., l$, such that

$$Zero(PS/DS) = \cup_{i=1}^{l} Zero(PD(ASC_i)/DS)$$

and that (a) there exist no i, j, $i \neq j$ such that $PD(ASC_i) \subset PD(ASC_j)$; (b) for all $d \in DS$ and $i = 1, ..., l$, $prem(d, ASC_i) \neq 0$.

Proof. See [23]. For our implementation of the algorithm, see [3]. ∎

3 The Theory of Resolvents

3.1 Properties of Resolvents

An ideal distinct from (1) and (0) is called *nontrivial.*

Definition 3.1. Let ID be a nontrivial ideal in $K[X]$. We can divide the x into two groups, $u_1, ..., u_q$ and $y_1, ..., y_p$, $p + q = n$, such that $ID \cap K[u_1, \cdots, u_q] = \emptyset$, while, for $i = 1, ..., p$, ID contains a nonzero polynomial in y_i and the u alone. We call the u a *parameter set* of ID.

In what follows in this section, we assume that ID is a non-trivial ideal in $K[U, Y]$ where the u consists of a parameter set of ID.

Lemma 3.2. A char set of ID under the variable order $u_1 < ... < u_q < y_1 < ... < y_p$ is of the form

$$ASC = A_1(u, y_1), A_2(u, y_1, y_2), ..., A_p(u, y_1, ..., y_p) \tag{3.2.1}$$

where A_i is a polynomial involving y_i effectively. Conversely, for an irreducible asc chain like (3.2.1), the u consist of a parameter set of the prime ideal $PD(ASC)$.

Proof. Let A_1 be a polynomial of y_1 and the u in ID with lowest degree in y_1, and ID_1 be the polynomials of y_1, y_2 and the u in ID whose degrees in y_1 are less than the degree of A_1 in y_1. ID_1 is not empty, because by the definition of the u there is a polynomial P of the u and y_2 in ID and P is obviously in ID_1. It is also clear that of the polynomials in ID_1 involving y_2 effectively, A_1 is of lowest degree in y_1. Let A_2 be a polynomial in ID_1 with lowest degree in y_2. Let $ID_2 \subset K[U, y_1, y_2, y_3] \cap ID$ such that the polynomials in ID_2 are of lower degrees in y_i than A_i , $i = 1, 2$. Continuing this procedure, at last we obtain an asc chain ASC. For any polynomial $P \in ID$, $R = prem(P, ASC)$ is of lower degree in y_i than the degree of y_i in A_i hence must be zero, i.e. ASC is a char set of ID. To prove the second part, first let us note it is obvious that $PD(ASC) \cap K[U] = \emptyset$. For any $i \leq p$, since $prem(A_i, A_1, \cdots, A_{i-1}) = A_i \neq 0$ by Lemma 2.4 there is a nonzero polynomial $P \in K[u, x_i]$ such that $P \in Ideal(A_1, \cdots, A_i)$. Thus the u are a parameter set of $PD(ASC)$. ∎

Lemma 3.3. The u are a parameter set of an ideal ID iff we have a decomposition

$$Zero(ID) = \cup_{i=1}^{t} Zero(PD(ASC_i)) \bigcup Zero(D') \quad (t > 0) \tag{3.3.1}$$

where each ASC_i is an irreducible asc chain with the u as a parameter set and D' is a polynomial set which contains nonzero u-pols.

Proof. It is a direct consequence of Theorem 4.5 in [4]. ∎

Corollary 3.3.1. In terms of ideals, (3.3.1) can be expressed as

$$Radical(ID) = \cap_{i=1}^{t} PD(ASC_i) \cap RD' \quad (t > 0)$$

where ASC_i is the same as in Lemma 3.3 and $RD' = Radical(D')$ is the radical ideal generated by D'.

The following lemma is crucial to the construction of the resolvents.

Lemma 3.4. Let ID be an ideal in $K[U, X]$ with the u as a parameter set. For a new variable w, there exist integers $M_1, ..., M_p$, and a u-pol G, such that two distinct zeros of ID with the u taking the same values for which G does not vanish give different values for $Q = M_1 y_1 + ... + M_p y_p$.

Proof. Let ID' be the ideal obtained from ID by replacing each y_i by a new variable z_i. Using p more new indeterminates λ_1, ..., λ_p, we consider the ideal

$$\Delta = Ideal(ID \cup ID' \cup \{\sum_{i=1}^{p} \lambda_i (y_i - z_i)\}).$$

As Δ contains ID, Δ has, for each $j \leq p$, a nonzero polynomial B_j in y_j and the u alone. Similarly, let C_j, $j = 1, ..., p$, be a nonzero polynomial of Δ in z_j and the u alone. Let D be the product of the initials of the B and C. Then D is a u-pol. For a zero of Δ for which $(y_1 - z_1)D \neq 0$, we have

$$\lambda_1 = -\frac{\lambda_2(y_2 - z_2) + ... + \lambda_p(y_p - z_p)}{y_1 - z_1}.$$

Let m be the maximum of the degrees of the B_i in the y_i and of the degrees of the C_j in the z_j. Let k be any positive integer. We write, for $s = 1, ..., k$ and for the above zero,

$$\lambda_1^s = \frac{E_s}{(y_1 - z_1)^k}$$

where E_s is a polynomial. Using the relations $B_i = 0$ and $C_j = 0$, we can depress the degree of E_s in each y_i and in each z_j to be less than m. The new expression of λ_1^s will be of the form

$$\lambda_1^s = \frac{F_s}{(y_1 - z_1)^k D_s}$$

where D_s is a product of powers of the initials of the B_i and C_j. Let L be the least common multiple of the D_s. We write

$$\lambda_1^s = \frac{H_s}{(y_1 - z_1)^k L}, s = 0, ..., k$$

with each H_s being a polynomial of degree less than m in y and z. The number of power products of the y_i and z_j, of degree less than m in each y and z, is m^{2p}. Consequently, if we take $k \geq m^{2p}$ and treat the power products of the y and z as independent variables, by eliminating these power products, we can find a nonzero polynomial in λ_1, of degree not greater than k, whose coefficients are polynomials in $\lambda_2, ..., \lambda_p$ and the u, which vanishes for every zero of Δ that does not annul $(y_1 - z_1)D$. Let K_1 be the product of this polynomial by D. Then K_1 vanishes for every zero of Δ that does not annul $y_1 - z_1$.

Similarly, for $i = 2, ..., p$, we can find a K_i which vanishes for every zero of Δ that does not annul $y_i - z_i$. We can find integers M_i, $i = 1, ..., p$, which, when substituted for the λ_i in $\prod_{1 \le i \le p} K_i$, reduce that polynomial to a nonzero polynomial G in the u. Any such set of M_i will furnish a Q as in the lemma. Because if two distinct zeros (u', y') and (u', y'') of ID give the same value for Q, then $(u', y', y'', M_1, ..., M_p)$ is a zero of Δ. Since $y'' \neq y'$ $G(u')$ must be zero. ∎

For a new indeterminate w, let $ID_1 = Ideal(ID, w - Q)$ where Q is the same as in Lemma 3.4. Then ID_1 is an ideal in $K[U, w, Y]$ and $ID_1 \cap K[U, Y] = ID$.

Lemma 3.5. The u consist of a parameter set of ID_1.

Proof. Since the u consist of a parameter set of ID, by Lemma 3.3, we have

$$Zero(ID) = \cup_{i=1}^{t} Zero(PD(ASC_i)) \bigcup Zero(D') \quad (t > 0)$$

where ASC_i are asc chains with the u as parameter set. Since $ID_1 = Ideal(ID, w - Q)$,

$$Zero(ID_1) = \cup_{i=1}^{t} Zero(PD(ASC_i) \cup \{w - Q\}) \bigcup Zero(D' \cup \{w - Q\}).$$

Under the variable order $u_1 < \ldots < y_p < w$, $ASC_i, w - Q$ is a (weak) asc chain. It is easy to show that $Ideal(PD(ASC_i) \cup \{w - Q\}) = PD(ASC_i, w - Q)$. Using Lemma 3.3 again, we know the u are a parameter set of ID_1. ∎

Theorem 3.6. Use the same notations as above. If ID is a prime ideal then a char set of ID_1 under the variable order $u_1 < ... < u_q < w < y_1 < ... < y_p$ is of the form

$$A(u, w), A_1(u, w, y_1), ..., A_p(u, w, y_p) \tag{3.6.1}$$

where A is an irreducible polynomial in w and $A_i = I_i(u) y_i - V_i(u, w)$.

Proof. By Lemma 3.5, the u consist of a parameter set of ID_1. By Lemma 3.2, a char set of ID_1 is of the form (3.6.1) except that we need to show $A_i = I_i(u) y_i - V_i(u, w)$. If an A_i is not linear in y_i, then by the procedure of constructing the generic point, (3.6.1) has two generic points, say g_1 and g_2, which have the same value for the u and w. Since g_1 and g_2 do not vanish the G (because G is a u-pol and the the value of the u in g_1 and g_2 are indeterminates) in Lemma 3.4 and they have the same value for the u and w, by Lemma 3.4, they are identical. This is a contradiction. Therefore, $A_i = I_i(u, w) y_i - V_i(u, w)$. By Lemma 2.5, we can further assume that I_i are free of the w. ∎

We call $A = 0$ a *resolvent* of the prime ideal ID. For the general case, we have

Theorem 3.7. Let ID be an ideal in $K[U, X]$ with the u as a parameter set and ID_1 be defined as above. A char set of *Radical*(ID_1) under the variable order $u_1 < ... < u_q < w < y_1 < ... < y_p$ is of the form

$$A(u, w), A_1(u, w, y_1), ..., A_p(u, w, y_p) \tag{3.7.1}$$

where $A_i = I_i(u)y_i - V_i(u,w)$.

Proof. By Lemma 3.5, the u consist of a parameter set of ID_1. Then they also consist of a parameter set of $Radical(ID_1)$. By Lemma 3.2, a char set of $Radical(ID_1)$ under the variable order $u < w < y_1 < ... < y_p$ is of form (3.7.1) except that we need to prove that A_i is linear in y_i. By Corollary 3.3.1,

$$Radical(ID_1) = \cap_{i=1}^{t} PD(ASC_i) \cap RD' \tag{3.7.2}$$

where $PD(ASC_i)$ are prime ideals with the u as parameter sets and RD' is a radical ideal containing a u-pol. We can further assume that there exist no $i \neq j$ such that $PD(ASC_i) \subset PD(ASC_j)$. By the selection of the M_i in Lemma 3.4, different zeros of $PD(ASC_i)$ with the same u which do not annul G give distinct values for Q. Thus by Theorem 3.6, a char set of $Ideal(PD(ASC_i), \{w - Q\})$ under the variable order $u < w < y_1 < ... < y_p$ is of the form

$$R_i(u,w), R_{i,1}(u,w,y_1), ..., R_{i,p}(u,w,y_p)$$

where each R_i is an irreducible polynomial and $R_{i,j} = I_{i,j}(u)y_j + V_{i,j}(u,w)$. We shall prove that $R_i \neq R_j$ for $i \neq j$. If this is not true, say $R_1 = R_2$, then by the selection of the M_i, a generic zero of ASC_1 must be the same as a generic zero of ASC_2 if they have the same value for w. Therefore $PD(ASC_1) = PD(ASC_2)$, which is impossible.

Let H be a u-pol in RD'. From (3.7.1) and (3.7.2), it is clear that $A = H\prod_{i=1}^{t} R_i$. We shall prove that there is a polynomial $A_i = I_i(u)y_i - V_i(u,w)$ in $Radical(ID_1)$. If this is true then $A, A_1, ..., A_p$ is a char set of $Radical(ID_1)$ and we have proved the theorem. We need only to show the case for $t = 2$. The general case can be proved similarly. Without loss of generality, we assume $I_{1,i} = I_{2,i}$. (Otherwise we may consider $I_{2,i}R_{1,i}$ and $I_{1,i}R_{2,i}$ instead of $R_{1,i}$ and $R_{2,i}$.) If $V_{1,i} = V_{2,i}$, then $A_i = HR_{1,i} = HR_{2,i}$ are in $Radical(ID_1)$. We have completed the proof. Otherwise, let R be the resultant of R_1 and R_2 w.r.t w. Then R is a nonzero u-pol and there exist polynomials B_1 and B_2 in $K[U,w]$ such that $R = B_1R_1 - B_2R_2$. Let

$$R_1' = U(R(J_1y_i + V_1) - B_1R_1(V_1 - V_2)), \quad R_2' = U(R(J_2y_i + V_2) - B_2R_2(V_1 - V_2))$$

where U is a u-pol in RD'. Then $R_1' - R_2' = H(R(V_1 - V_2) - (V_1 - V_2)(B_1R_1 - B_2R_2)) = 0$, i.e., $R_1' = R_2'$ are in $PD(ASC_1) \cap PD(ASC_2)$. Since $H \in RD'$, R_1' is in $Radical(ID_1)$ by (3.7.2). We have completed the proof. ∎

We call the equation $A = 0$ a *resolvent* of ID w.r.t the u. Note that the proof of Theorem 3.7 actually provides more information:

Corollary 3.7.1. For an irredundant decomposition (3.3.1) of ID, we have

(1) For the same Q, the resolvents of $PD(ASC_i)$ are mutually different and the resolvent of ID w.r.t the u is the product of the resolvents of $PD(ASC_i)$, $i = 1, ..., t$, and an appropriate u-pol.

(2) We have a method to construct a char set of $Radical(ID)$ if char sets for $PD(ASC_i)$, $i = 1, \cdots, t$ are known.

3.2 Methods of Constructing Resolvents

To find a resolvent of an ideal ID w.r.t a set of parameters, we first express $Radical(ID)$ as intersection of prime ideals, then find the resolvent for each prime ideal, finally construct a resolvent for ID from these resolvents.

Algorithm 3.8. Let PS be a finite set of polynomials in $K[u_1, ..., u_q, y_1, ..., y_p]$. The algorithm decides whether the u are a parameter set of $ID = Ideal(PS)$, and if it is, finds a resolvent of ID w.r.t the u.

Step 1. By Theorem 2.6, under the variable order $u < y_1 < ... < y_p$, we have

$$Zero(PS) = \cup_{i=1}^{l} Zero(PD(ASC_i)) \bigcup \cup_{j=1}^{t} Zero(PD(ASC_j^*))$$

where the ASC_i, $i = 1, ..., l$, are all the asc chains in the decomposition which have the u as their parameter sets. Then by Lemma 3.3, the u are a parameter set of ID iff $l > 0$ and there exist at least one u-pol in each ASC_j^*. If this is the case, go to Step 2. Otherwise the algorithm stops.

Step 2. Let $\lambda_1, ..., \lambda_p, w$ be new indeterminates and let $ID_1 = Ideal(PS, w - Q)$ be an ideal in $K[U, \lambda, w, Y]$, where $Q = \lambda_1 y_1 + ... + \lambda_p y_p$. By Lemma 3.5, ID_1 is an ideal with the u and the λ as a parameter set.

Step 3. For each $i = 1, ..., l$, by Algorithm 3.10, we find a char set

$$A_i(\lambda, u, w), A_{i,1}(\lambda, u, w, y_1), ..., A_{i,p}(\lambda, u, w, y_p)$$

for the prime ideal $Ideal(PD(ASC_i), w - Q)$ under the variable order $l < u < w < y_1 < ... < y_p$. As the λ are arbitrary indeterminates, by the proof of Lemma 3.4 and Theorem 3.6, $A_{i,j}$ are linear in y_j. By (1) of Corollary 3.7.1, $A_i \neq A_j$ for $i \neq j$.

Step 4. By (2) of Corollary 3.7.1, we can construct a char set for $Radical(ID_1)$

$$R(l, u, w), R_1(l, u, w, y_1), ..., R_p(l, u, w, y_p) \tag{3.8.1}$$

where $R_i = I_i(l, u)y_i - V_i(l, u, w)$. Let $D = I \prod_{i=1}^{p} I_p$ where I is the initial of R. Then D is a polynomial of the u and the λ.

Step 5. Let $a_1, ..., a_p$ be integers, for which D becomes a nonzero polynomial in the u and $A_i \neq A_j$ is still true, when each λ_i is replaced by a_i. For $\lambda_i = a_i, i = 1, ..., p$, (3.8.1) becomes

$$R'(u, w), R'_1(u, w, y_1), ..., R'_p(u, w, y_p) \tag{3.8.2}$$

We assume that the u-pol factors of R' have been removed.

Step 6. By Lemma 3.9, R' is a resolvent of $Ideal(PS)$.

Lemma 3.9. (3.8.2) is a char set of $Radical(ID_2)$ where $ID_2 = Ideal(PS \cup \{w - \sum_i a_i y_i\})$.

Proof. If (3.8.2) is not a char set of $Radical(ID_2)$, $Radical(ID_2)$ will have a char set $T, T_1, ..., T_p$ with T of lower degree g in w than R' and T_i are linear in y_i. We can assume that the initials of the T_i are free of w since such polynomials exist in $Radical(ID_2)(i.e., R_i')$. If D is the product of those initials, we have, for a zero of ID_2 in which the values of the u are independent indeterminates,

$$y_i = \frac{C_{i,g-1}w^{g-1} + ... + C_{i,0}}{D} \tag{3.9.1}$$

where the C are u-pols. Let us consider the ideal $ID_3 = Ideal(PS, v - \lambda_1 y_1 - ... - \lambda_p y_p)$ in $K[U, \lambda, v, Y]$ for a new indeterminate v. We will show that ID_3 contains a nonzero polynomial P, free of the y, which is of degree no more than g in v. This polynomial is also in $Radical(ID_3)$. Noting that $Radical(ID_1)$ and $Radical(ID_3)$ should have char sets in which the first polynomials of both char sets have the same degree. We thus get a contradiction.

We consider the relations

$$v^i = (\lambda_1 y_1 + ... + \lambda_p y_p)^i, \qquad i = 1, ..., g.$$

We replace the y by their expression in (3.9.1) and depress the degrees in w of the polynomials on the right side to less than g, using the relation $T = 0$. We have such get a set PS of g polynomials of the u, the λ, v, and w such that the polynomials in PS are of degree less than g in w and of degree no more than g in v. Treating w, w^2, ..., w^{g-1} as independent variables in the polynomials in PS, we eliminate them and get a nonzero polynomial Q in v, the u and the λ. Note that the special position of the v^i in the polynomials of PS, Q is of degree no more than g in v. We have completed the proof. ∎

Algorithm 3.10. Let $ASC = A_1, ..., A_p$ be an irreducible asc chain in K[U,Y] where the u are a parameter set of ASC. The algorithm finds a char set for the prime ideal $D = Ideal(PD(ASC) \cup \{w - Q\})$ under the variable order $l < u < w < y_1 < \cdots < y_p$, where $Q = \lambda_1 y_1 + ... + \lambda_p y_p$.

Step 1. By Theorem 2.6, under the variable order $u < \lambda < w < y_1 < \ldots < y_p$ we have

$$Zero(ASC \cup \{w - Q\}) = \cup_{i=1}^{t} Zero(PD(ASC_i')). \tag{3.10.1}$$

Step 2. By (2.1), we have

$$Zero(ASC) = Zero(PD(ASC)) \bigcup \cup_{i=1}^{p} Zero(ASC \cup \{init(A_i)\})$$

By Lemma 2.4, there is a polynomial $U_i \in Ideal(ASC \cup \{init(A_i)\})$ which involves the u and the λ alone. Thus, there is only one irreducible component in $Zero(ASC \cup \{w - Q\})$, i.e., $Zero(D)$, on which the u and l are algebraically independent.

Step 3. Therefore only one component in (3.10.1), say $Zero(PD(ASC_1'))$, with the u and l as a parameter set and ASC_1' is a char set of D.

Step 4. By Lemma 2.5, we can assume that the initials of the polynomials in ASC_1' involve the u alone. ∎

We have the following variations for Algorithm 3.8 and Algorithm 3.10.

Modification 3.11. For Algorithm 3.10, we can use the Gröbner basis method instead of Theorem 2.6 to compute a char set of D as follows. Let GB be a Gröbner basis of $Ideal(PS')$ ($PS' = ASC \cup \{w - Q\}$) in $K(l, U)[w, Y]$ in purely lexicographic order $w < y_1 < \ldots < y_p$ (for the Gröbner basis method, see [2]). As in $K(l, U)[w, Y]$, $Ideal(ASC_1 \cup \{w - q\})$ defines a zero dimensional prime ideal, then GB is also a char set of $Ideal(PS')$ (see [8] or [5]).

Modification 3.12. In practice, Algorithm 3.8 may be very slow, because by introducing new variables λ_i, large polynomials could be produced in the procedure. An idea to improve the efficiency is that we can randomly select p integers $a_1, ..., a_p$ and use $Q' = w - a_1y_1 - ... - a_py_p$ instead of $Q = w - \lambda_1y_1 - ... - \lambda_py_p$ to compute the resolvent, i.e., we compute char sets of $Radical(PS, w - Q')$ directly by using methods similar to those in Algorithm 3.8. The success probability of the selection of the integers should be one, because by Step 5 of Algorithm 3.8, the integers which do not suit for the above purpose consist of an algebraic set of lower dimension than q.

4 Applications of the Resolvents

4.1 A Hypersurface Birational to a Variety

It is well known in algebraic geometry [13] that:

Theorem 4.1. Any irreducible variety of dimension r is birational to a hypersurface in E^{r+1}.

We will prove the following more general result.

Theorem 4.2. Let PS be a finite polynomial set in $K[U, Y]$ such that the u are a parameter set of $Ideal(PS)$ and no prime component of $Radical(PS)$ contains a nonzero u-pol. Then we can find a polynomial R of w and the u such that $Zero(PS)$ is birational to $Zero(R)$. The birational maps can also be found.

Proof. By Algorithm 3.8, we can find integers $M_1, ..., M_p$ such that a char set of $RD = Radical(PS \cup \{w - (M_1y_1 + ... + M_py_p)\})$ is of the form

$$R(u, w), R_1(u, w, y_1), ..., R_p(u, w, y_p) \tag{4.2.1}$$

where $R_i = I_iy_i - U_i$ (I_i are u-pols) and $R = 0$ is a resolvent for $Ideal(PS)$. We define a morphism

$$MP_1 : Zero(PS) \to Zero(R)$$

by setting $MP_1(u_1, ..., u_q, y_1, ..., y_p) = (u_1, ..., u_q, M_1y_1 + ... + M_py_p)$. We define another morphism

$$MP_2 : Zero(R) \to Zero(PS)$$

by setting $MP_2(u_1, ..., u_q, w) = (u_1, ..., u_q, U_1/I_1, ..., U_p/I_p)$. Let $I = \prod_{i=1}^{p} I_i$. Then MP_2 is well defined on $D_1 = Zero(R) - Zero(I)$. Since no component of $Radical(PS)$ contains a nonzero u-pol, $Radical(PS) = \cap PS_i$ where PS_i are prime ideals whose parameter sets are the u. By Corollary 3.7.1, R is a polynomial with no factor involving the u alone. Therefore MP_2 is well defined on $Zero(R)$ except a part $Zero(I)$ with lower dimension than q. We may check that $MP_1(MP_2)$ and $MP_2(MP_1)$ are identity maps. Therefore, $Zero(R)$ and $Zero(PS)$ are birational. The birational maps between them are MP_1 and MP_2. ∎

Corollary 4.3. Let PS be a finite polynomial set in $K[U, Y]$ such that the u are a parameter set of $Ideal(PS)$. Then we can find a polynomial R of w and the u and a u-pol H such that $Zero(PS/H)$ is birational to $Zero(R/H)$.

Proof. By Lemma 3.3, $Zero(PS) = \cup_i Zero(PS_i) \cup Zero(D)$ where PS_i are prime ideals whose parameter sets are the u and D is an ideal containing a nonzero u-pol, say H. Then $Zero(PS/H) = \cup_i Zero(PS_i/H)$. Then the result can be proved similarly as Theorem 4.2. ∎

4.2 Parameterization of Algebraic Curves

An irreducible *algebraic curve* is an irreducible variety of dimension one. Let $C = Zero(PS)$ be an irreducible algebraic curve where $PS \subset K[X]$. Then C is called *rational* if there exist polynomials $u_1, ..., u_n, w$ of an indeterminate t such that $gcd(u_1, ..., u_n, w) = 1$ and $\forall P \in PS$, $P(u_1/w, ..., u_n/w) \equiv 0$. We call

$$x_1 = u_1/w, \cdots, x_n = u_n/w$$

a set of *parametric equations* for the curve. The maximum of the degrees of u_i and w is called the degree of the parametric equations.

In this section, we give a decision method to find whether an algebraic curve is rational, and if it is, to find a set of parametric equations for it. See [10] for more details. For other methods of parameterizing curves, see [1] and [20].

As a special case of constructing resolvents, we have

Theorem 4.4. For an irreducible algebraic curve $C = Zero(PS)$ in A^n, we can find an irreducible polynomial of two variables $f(x, y)$ such that C is birational to $Zero(f)$. The birational maps between C and $Zero(f)$ can also be obtained.

It is obvious that C is rational iff $f(x, y) = 0$ is rational. Furthermore, using the birational transformations between C and $f = 0$, we can find a set of parametric equations for C (or $f = 0$) if a set of parametric equations of $f = 0$ (or C) is given. Hence, we need only to find a set of parametric equations for $f(x, y) = 0$.

Definition 4.5. A set of parametric equations $x = u_i/w$ for a curve C is called *proper* if, except for a finite number of points, for each point $(x'_1, ..., x'_n)$ on C there only exists one value t_0 for t such that $x'_i = u_i(t_0)/w(t_0), i = 1, ..., n$.

A rational curve always has a set of proper parametric equations [21].

Theorem 4.6. Let $x = u(t)/w(t), y = v(t)/w(t)$ be a set of proper parametric equations for a plane curve $f(x, y) = 0$. We assume $gcd(u, v, w) = 1$. Then the degree of f is the same as the degree of the parametric equations.

Proof. Let f be of degree d and the parametric equations be of degree d'. By Bezout's theorem [21], the degree of $f = 0$ equals the number of the intersection points between $f = 0$ and a generic straight line. Let $ax + by - 1 = 0$ be the equation of a generic line where a and b are indeterminates. The parametric values corresponding to the intersection points are the roots of the equation $P(t) = au(t) + bv(t) - w(t) = 0$. Then $d \leq d'$. Since $gcd(u, v, w) = 1$, $P(t)$ is irreducible. Thus $P(t) = 0$ has d' distinct roots. Since the parametric equations are proper, we have $d' \leq d$. ∎

Algorithm 4.7. Let PS be a finite set of polynomials in K[X]. The algorithm decides whether $C = Zero(PS)$ is a rational irreducible algebraic curve, and if it is, finds a set of parametric equations for C.

Step 1. By Theorem 2.6, we have an irredundant decomposition

$$Zero(PS) = \cup_{i=1}^{m} Zero(PD(ASC_i)).$$

C is an irreducible algebraic curve iff $m = 1$ and ASC_1 contains $n - 1$ polynomials. If this is the case, go to Step 2. Otherwise, the algorithm terminates.

Step 2. We rename the parameter of ASC_1 as u_1. Other variables are also renamed so that $ASC_1 = A_1(u_1, y_1), ..., A_p(u_1, y_1, ..., y_p)$, $p = n - 1$.

Step 3. By Algorithm 3.8, we can find a resolvent $f(x, y) = 0$ of degree d for $PD(ASC_1)$ and birational transformations between $Zero(f)$ and $Zero(PD(ASC_1))$.

Step 4. Let

$$x = u(t)/w(t), y = v(t)/w(t) \tag{4.7.1}$$

where $u(t) = u_d t^d + ... + u_0$, $v(t) = v_d t^d + ... + v_0$, and $w(t) = w_d t^d + ... + w_0$ for indeterminates u_i, v_i, and w_i.

Step 5. Replacing x and y by $u(t)/w(t)$ and $v(t)/w(t)$ in $f(x, y) = 0$ and clearing the denominators, we obtain a polynomial Q of t whose coefficients are polynomials of u_i, v_i and the w_i. Let the set of coefficients of Q as a polynomial of t be $HS = \{P_1, ..., P_h\}$.

Step 6. (4.7.1) is a set of parametric equations for $f = 0$ iff HS has a set of zeros such that when the coefficients of u, v, and w are replaced by these zeros, $u(t)/w(t)$ and $v(t)/w(t)$ are not numbers in K.

Step 7. Let $DS_1 = \{u_i w_j - u_j w_i \mid i, j = 1, ..., d\}$, $DS_2 = \{v_i w_j - v_j w_i \mid i, j = 1, ..., d\}$. Then $f = 0$ is rational iff $HD = Zero(HS) - (Zero(DS_1) \cup Zero(DS_2))$ is not empty, and if it is not empty, each zero of HD provides a set of parametric equations for $f = 0$. ∎

In the above algorithm, we have to solve a system of algebraic equations. We can use the method based on Wu-Ritt's decomposition algorithm [24]. This method is complete in the field of complex numbers. If one wants to find real coefficients parametric equations, we have to find the real zeros of a set of polynomials, which can be done by Collin's CAD method [6].

4.3 The Primitive Elements of Algebraic Extension Fields

A basic result in algebraic extension theory is that there exists a primitive element in each finite algebraic extension of a field of characteristic zero. Precisely, we have

Theorem 4.8. Let η_1, ..., η_m be algebraic over K. Then there exist $f_i \in K$, $i = 1, ..., m$, such that $K(\zeta) = K(\eta_1, ..., \eta_m)$ where $\zeta = \sum_{i=1}^m f_i\eta_i$.

We consider the following more general problem.

Theorem 4.9. Let η_1 be algebraic over K and for $i = 2, ..., m$, η_i be algebraic over $K_{i-1} = K(\eta_1, ..., \eta_{i-1})$. Then we can find integers f_i, $i = 1, ..., m$, such that if $\zeta = \sum_{i=1}^m f_i\eta_i$ then $K(\zeta) = K_m$.

Proof. We assume that the η_i are given by the following sequence of polynomials

$$A_1(x_1), A_2(x_1, x_2), ..., A_m(x_1, ..., x_m)$$

i.e., $A_i(\eta_1, ..., \eta_i) = 0$, $i = 1, ..., m$. Without loss of generality, we assume the initial of each A_i is a nonzero number in K. In this case, $ID = Ideal(A_1, ..., A_m)$ defines a zero dimensional variety, i.e. the parameter set of ID is empty. Then by Algorithm 3.8, we can find integers f_i, $i = 1, ..., m$, such that a char set of $Radical(ID, w - \sum_{i=1}^m f_ix_i)$ under the variable order $w < x_1 < ... < x_m$ is of the form

$$R(w), R_1(w, x_1), ..., R_m(w, x_m)$$

where $R_i = x_i - U_i(w)$. Replacing x_i by η_i in R_i, we have $\eta_i = U(\zeta)$, i.e., $K(\zeta) = K_m$. ∎

4.4 Solving Systems of Polynomial Equations

Let PS be a finite polynomial set in $K[X]$ with a finite number of zeros for the x. Then $Ideal(PS)$ is of dimension zero and has an empty parameter set. Thus, by Algorithm 3.8, we can find integers $m_1, ..., m_n$ such that a char set of $Radical(PS \cup \{w - m_1x_1 - ... - m_nx_n\})$ under the variable order $w < x_1 < ... < x_n$ is of the form

$$R(w), R_1 = x_1 - U_1(w), ..., R_n = x_n - U_n(w) \tag{4.8}$$

where U_i are univariate polynomials with degree less than $degree(R(w))$. Then the distinct zeros of $Ideal(PS)$ can be obtained as follows

$$Zero(PS) = \{(x_1, \cdots, x_n) \ : \ x_i = U_i(w), i = 1, \cdots, n, R(w) = 0\}.$$

Conversely,

$$Zero(R(w)) = \{\sum_{i=1}^{n} m_i x_i \ : \ (x_1, \cdots, x_n) \in Zero(PS)\}.$$

As a conclusion, there is a one to one correspondence between the real (complex) roots of $R(w)$ and the real (complex) distinct zeros of PS.

Let $R(w)$ be of degree N. Then U_i must be of degree less than N. To find the zeros of PS, we need only to find the roots of $R(w)$ and solvers for univariate polynomials are widely available [7]. Now we have the following result on error estimation.

Lemma 4.10. If w_0 is a root of $R(w) = 0$ and w' is a number such that $|w_0 - w'| < \epsilon < 1$, we have $|U_i(w_0) - U_i(w')| < \epsilon \frac{(M+2m)^{N+1}}{m^N}$, where M and m are the maximal and minimal absolute values of the coefficients of $R(w)$ and U_i, $i = 1, ..., n$.

Proof. Since $R(w_0) = 0$, $\|w_0\| < C = 1 + M/m$ [18]. Let $\delta = w' - w_0$. Since $|w_0 - w'| < \epsilon < 1$, we have $\delta \leq 1$. We have $|w'^k - w_0^k| = |(w_0 + \delta)^k - w_0^k| \leq \delta \cdot |k w_0^{k-1} + ... + \delta^k| \leq \delta \cdot ((C+1)^k - C^k) \leq \delta (C+1)^k < \epsilon (C+1)^k$. Then $|U_i(w_0) - U_i(w')| \leq M(|w'^{N-1} - w_0^{N-1}| + ... + |w' - w_0|) \leq \epsilon M((C+1)^{N-1} + ... + (C+1)) < \epsilon M(C+1)^N/(C-1) \leq \epsilon M(C+1)^N = \epsilon M(M+2m)^N/m^N \leq \epsilon (M+2m)^{N+1}/m^N$. ∎

As a conclusion, we have

Theorem 4.11. Let $e_1, \cdots, e_s$ be rational approximate roots of $R(w) = 0$ with accuracy $\epsilon < \delta \frac{m^N}{\sqrt{n}(M+2m)^{N+1}}$ for a positive number $\delta < 1$. Then $(U_1(e_i), \cdots, U_n(e_i))$, $i = 1, \cdots, n$, are δ approximations of the zeros of PS.

Proof. Let $w_1, \cdots, w_s$ be the roots of $R(w) = 0$ corresponding to $e_1, \cdots, e_s$. By Lemma 4.10,

$$\sqrt{\sum_{k=1}^{n} (U_k(w_i) - U_k(e_i))^2} < \epsilon \sqrt{n} \frac{(M+2m)^{N+1}}{m^N} < \delta. \quad ∎$$

We will go further to isolate the real (complex) zeros of PS, i.e., we need to find disjoint regions in R^n (or C^n in the case of finding the complex zeros), each containing exactly one real (complex) zero of PS.

Let us assume that we have obtained the asc chain (4.8). We always exclude the trivial case whose $R(w)$ is linear. We also exclude the trivial case where U_i is a constant. Let $V_i(x_i)$, $i = 1, \cdots, n$, be the resultant of $A(w)$ and $U_i(w) - x_i$ for the variable w. Then it is clear that the zeros of $V_i(x_i) = 0$ are the projections of $Zero(PS)$ upon the i-th axis of R^n. Since (4.8) is the characteristic set of a radical ideal, V_i must be square free. We also assume that $R(w)$ and V_i are integral, i.e., their coefficients are integers.

Theorem 4.12. Let $e_1, \cdots, e_t$ be rational approximate roots of $R(w) = 0$ with accuracy $\epsilon < s \frac{m^N}{8\sqrt{n}(M+2m)^{N+1}}$ where M and m are the maximal and minimal absolute values of the coefficients of $R(w)$ and U_i, $i = 1, ..., n$; $s = \sqrt{3} 2^{\frac{1-N}{2}} N^{-N} T^{1-N}$; and T is the maximal absolute value of the coefficients of $V_i(x_i)$. Then the spheres with $(U_1(e_i), \cdots, U_n(e_i))$, $i = 1, \cdots, t$, as centers and with radius $\frac{s}{8}$ are disjoint and each contains exactly one zero of PS.

Proof. First, let us note that $1 \le degree(V_i(x_i)) \le N$, because PS has only N different zeros. Since $R(w)$ and $V_i(x_i)$ are integral and $degree(R(w)) \ge 2$, from (p.362, [18]), we know that a lower bound for the distances among the roots of V_i is

$$\begin{aligned} s_i &= \sqrt{3} d_i^{-\frac{d_i+1}{2}} (\sum_{i=0}^{d_i} c_i^2)^{\frac{1-d_i}{2}} \ge \sqrt{3} d_i^{-\frac{d_i+1}{2}} ((d_i+1)T^2)^{\frac{1-d_i}{2}} \\ &\ge \sqrt{3} 2^{\frac{1-d_i}{2}} d_i^{-d_i} T^{1-d_i} \ge \sqrt{3} 2^{\frac{1-N}{2}} N^{-N} T^{1-N} \end{aligned}$$

where c_i, $i = 1, \cdots, d_i$ are the coefficients for $V_i(x_i)$. Then $s = \sqrt{3} 2^{\frac{1-N}{2}} N^{-N} T^{1-N}$ is a lower bound for the distances among the distinct zeros of PS. By Theorem 4.11, $Z_i = (U_1(e_i), \cdots, U_n(e_i))$, $i = 1, \cdots, t$, are the approximate zeros of PS with accuracy $\frac{s}{8}$. Therefore, each sphere with Z_i as center and with radius $\frac{s}{8}$ contains a zero of PS. Distinct spheres thus obtained are disjoint because the distance between two $\frac{s}{8}$-approximate zeros of PS must be $> \frac{3s}{4}$ and the distance between two distinct spheres must be $> \frac{s}{2}$. ∎

It is easy to rationalize the bounds in Theorems 4.11 and 4.12.

References

[1] S. S. Abhyankar and C. Bajaj, Computations with Algebraic Curves, *Proc. of ISSAC-89*, LNCS No. 358, pp. 274–284, Springer-Verlag, 1989.

[2] B. Buchberger, Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, in *Recent Trends in Multidimensional Systems theory* (ed. N.K. Bose), D.Reidel Publ. Comp., 1985.

[3] S.C. Chou and X.S. Gao, Ritt-Wu's's Decomposition Algorithm and Geometry Theorem Proving, *Proc. of CADE'10*, M.E. Stickel (Ed.), pp 207–220, LNCS, No. 449, Springer-Verlag, 1990.

[4] S.C. Chou and X.S. Gao, Mechanical Formula Derivation in Elementary Geometries, *Proc. ISSAC-90*, ACM, New York, 1990, pp. 265–270.

[5] S.C. Chou, W. Schelter, and G.J. Yang, "Characteristic Sets and Gröbner Bases in Geometry Theorem Proving", *Resolution of Equations in Algebraic Structure*, Vol. I, pp33–92, Academic Press, Boston, 1989.

[6] G. E. Collins, Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition, Lect. Notes Comp. Sci. 33, 134–183, Springer-Verlag, 1975.

[7] G. E. Collins and R. Loos, Real Zero of Polynomials. In *Computer Algebra*, edited by B. Buchberger et al. Springer-Verlag, New York, 1982.

[8] X.S. Gao, The Minimal Characteristic Basis of a Polynomial Ideal, *J. Sys sci & Math Scis*, No.2, 1989, 236-242.

[9] X.S. Gao, On the Theory of Resolvents and Its Applications, MM-Research Preprints, No.6, 1991, Inst. of Systems Science, Academia Sinica.

[10] X.S. Gao and S.C. Chou, On the Parameterization of Algebraic Curves, *Applicable Algebra in Elementary Communication and Computing*, **3**, 27–38, Springer-Verlag, 1992.

[11] P. Gianni amd T. Mora Algebraic Solution of Systems of Polynomial Equations Using Gröbnert bases, *Proc. of AAECC-5*, pp. 247–257, LNCS, No. 356, Springer-Verlag, 1987.

[12] C. Gallo and B. Mishra, Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets, Preprints, Courant Institute of Math. Sciences, 1989.

[13] R. Hartshorne, *Algebraic Geometry*, Springer-verlag, 1977.

[14] H. Kobayashi, S. Moritsugu and R.W. Hogan, Solving Systems of Algebraic Equations, *Proc. of ISSAC-88*, pp.139–149, LNCS No. 358, Springer-Verlag, 1988.

[15] Lazard, D. (1991). A New Method for Solving Algebraic Systems of Positive Dimension. *Discr. Applied Math.,* 33, p.147-160.

[16] Liu Zhuojun, An Algorithm on Finding All Isolated Zeros of Polynomial Equations, *MM Research Preprints*, No4, 1987, Ins. of Sys. Sci., Academia Sinica.

[17] G.K. Loos, Computing in Algebraic Extensions, in *Computer Algebra* (Ed. by B. Buchberger, et al), pp. 173–188, Springer-Verlag, 1982.

[18] M. Mignotte, Some Useful Bounds, in *Computer Algebra* (ed. by B. Buchberger et al), Springer-Verlag, 1982.

[19] J. F. Ritt, *Differential Algebra*, Amer. Math. Sco. Colloquium, (1950).

[20] J. R. Sendra and F. Winkler, Symbolic Parameterization Curves, *J. of Symbolic Computation*, **12**(6), 607–632, 1991.

[21] R. Walker, *Algebraic Curves*, Princeton Univ. Press, 1950.

[22] D. M. Wang, A Method of Factorizing Multivariate Polynomials Over Successive Algebraic Extension Fields, preprint, RISC-Linz, Kepler Univ., Austria, 1992.

[23] W. T. Wu, Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J. Sys. Sci. & Math. Scis.*, **4** (1984), 207–235.

[24] W. T. Wu, On Zeros of Zlgebraic Equations — An Applications of Ritt Principle, *Kexue Tongbao*, **31**(1986), 1–5.

[25] K. Yokoyama, M. Noro and T. Takeshima, Computing Primitive Elements of Extension Fields, *J. Symbolic Computation*, **8**, pp. 553–580, 1989.

[26] L. H. Zhi, Factorization of Polynomials over Algebraic Extension Fields and its Applications, PhD Thesis, 1996, Institute of Systems Science.